Date: 6/26/03 Express Mail Label No. EV 214934480US

Inventor: ChongLim Kim

Attorney's Docket No.: 3423.1004-001

METHOD AND SYSTEM FOR ENCRYPTING ELECTRONINC MESSAGE USING SECURE AD HOC ENCRYPTION KEY

RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Application No. 60/392,223, filed June 26, 2002, and U.S. Provisional Application No. 60/399,334, filed July 28, 2002. The entire teachings of the above applications are incorporated herein by reference.

BACKGROUND OF THE INVENTION

Encryption is useful to secure the contents of an electronic message end-to-end during transmission from a sender to a receiver. In asymmetric cryptography, encryption and decryption is done using a public-private key pair. In symmetric cryptography, encryption and decryption is done using one shared key. Symmetric cryptography is much more efficient computationally compared to asymmetric cryptography.

To encrypt a message such as an electronic mail using symmetric encryption, a shared key has to be agreed upon by the sender and the receiver. If both parties are able to authenticate each other, the sender can use a key negotiation protocol with the receiver to set up a secret shared key, but this still requires that the receiver be online at the time the sender needs to create the shared key for encrypting the message to the receiver. Or, the sender can securely distribute the shared key out-of-band to the

receiver, but this is often not practical because that step has to be done for every receiver that the sender wishes to communicate with. Furthermore, in situations where the sender sends multiple messages which are received in a batch by the receiver, the secret shared key may be accessed multiple times by the sender, which could increase the chance of the shared key being compromised.

To overcome the above problems, asymmetric cryptography may be employed. To encrypt a message such as an electronic mail, a shared key again may be used to encrypt the message plaintext into ciphertext. In this case however, the shared key itself is encrypted by the sender using the receiver's known public key and sent to the receiver along with the ciphertext. The shared key is decrypted by the receiver using the receiver's corresponding private key. The decrypted shared key is then used by the receiver to decrypt the ciphertext back into the message plaintext.

A public key infrastructure, PKI, has evolved whereby a certificate attached to a public key is used to attest that a particular public key is bound to or associated with a particular party. The certificate is created and digitally signed by a trusted public key certificate authority, CA, using the CA's private key. To digitally sign a certificate (or any message), the CA would calculate a hash function result for the certificate and encrypt the hash result using the CA's private key. The certificate and its encrypted hash result (digital signature) are attached to the public key and given to the receiver claiming ownership of the public-private key pair. The sender obtaining the receiver's public key verifies the digital signature of the certificate on the public key. This is done by decrypting the certificate's hash result using the CA's well-known public key and matching that with the hash function result calculated directly from the certificate.

However, if the receiver has not acquired a public-private key pair or has not publicized his/her public key, the sender is unable to encrypt the message utilizing the receiver's known public key. Acquiring and managing a public-private key pair appear to be too involved or too much bother in many instances, such as for electronic mail. A user has to go through a fairly involved process to generate a public-private key pair, and then another fairly involved process to obtain a certificate for the public key. A

user also has to protect the private key from being found out or stolen. Often the public-private key pair is stored on a user's primary computer, which is not accessible when the user is not using the primary computer. When a primary computer is replaced, the public-private key has to be exported from the old primary computer and imported into a new primary computer. Hence receiver acquisition of a public-private key pair and receiver key management are significant impediments and drawbacks. For the above reasons, among others, e-mail message encryption using PKI is not widely adopted in spite of the obvious security advantages.

A key server provides a method for generating and associating a new public-private key pair for a receiver when a public key that is associated with the receiver e-mail address is not known. However, the new private key of the public-private key pair is not cryptographically secure in the key server. Another related problem is that since the new key pair is publicized to be associated with the receiver e-mail address, a compromised private key of the public-private key pair can be used to digitally sign e-mail that is purported to come from the receiver. The receiver also may not want a public-private key pair that is generated by another party (i.e. sender) to be universally associated with the receiver e-mail address.

SUMMARY OF THE INVENTION

This invention relates to generating and using cryptographically secure ad hoc encryption keys to encrypt and decrypt electronic messages.

An object of the present invention is to allow a sender to generate an ad-hoc public-private key pair whose encrypted private key is known only to the sender in order to encrypt an e-mail message to a receiver without the receiver's involvement, when there is no known receiver public key for the sender to use, or the receiver is not online to participate in a key negotiation protocol to set up a shared key with the sender, or an out-of-band shared key distribution between the sender and the receiver is not practical, or it is more secure for the sender to be able to use a public key instead of accessing a stored secret shared key to encrypt the sender's multiple messages.

Another object of the present invention is for the ad-hoc public-private key pair generated by the sender without the receiver's involvement not to be universally associated with the receiver e-mail address.

A sender desiring to encrypt an electronic message prior to sending to a receiver generates an ad hoc public key and private key asymmetric key pair that is uniquely associated with both the sender and the receiver; encrypts the private key, the private key known only to the sender; creates an index value that is uniquely associated with the key pair, the index value utilized for key retrieval; stores in a key server at least the encrypted private key together with the associated index value; and encrypts the electronic message by utilizing the public key. In an alternative embodiment, the private key is encrypted symmetrically by utilizing a sender secret. In another embodiment, the index value is known only to the sender. In an alternative embodiment, an identity value is obtained by utilizing at least a unique identification for the sender and a unique identification for the receiver, and the index value is computed from the identity value by utilizing a sender secret. In another embodiment, the electronic message is an electronic mail message. In another embodiment, the key pair is a set of at least one key pair, each key pair associated with a validity field. In yet another embodiment, the ad hoc public key and private key asymmetric key pair is an ad hoc symmetric key.

A receiver desiring to decrypt an encrypted electronic message received from a sender authenticates the receiver to the sender; derives an index value that is uniquely associated with an ad hoc public key and private key asymmetric key pair, the key pair uniquely associated with both the sender and the receiver; retrieves an encrypted private key from a key server by utilizing the index value, the encrypted private key known only to the sender; and decrypts the encrypted electronic message by utilizing the encrypted private key. In an alternative embodiment, an unencrypted private key is obtained from the encrypted private key by utilizing a sender secret, and the encrypted electronic message is decrypted by utilizing the unencrypted private key. In another embodiment, the index value is known only to the sender. In an alternative

embodiment, an identity value is obtained by utilizing at least a unique identification for the sender and a unique identification for the receiver, and the index value is computed from the identity value by utilizing a sender secret. In another embodiment, the electronic message is an electronic mail message. In another embodiment, the key pair is a set of at least one key pair, each key pair associated with a validity field, and an encrypted private key retrieved and utilized for decrypting the encrypted electronic message, the encrypted private key selected from the set based on the associated validity field. In yet another embodiment, the ad hoc public key and private key asymmetric key pair is an ad hoc symmetric key.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features and advantages of the invention will be apparent from the following more particular description of preferred embodiments of the invention, as illustrated in the accompanying drawings in which like reference characters refer to the same parts throughout the different views. The drawings are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention.

Fig. 1 is a block diagram of a system for encrypting an electronic message according to the principles of present invention;

Fig. 2 is a flow diagram of a procedure for encrypting an electronic message according to the present invention;

Fig. 3 is a block diagram illustrating an identity value that can be used to compute an index value utilized for key retrieval in one embodiment;

Fig. 4 is a block diagram illustrating a set of key pairs with validity fields; and

Fig. 5 is a flow diagram of a procedure for decrypting an electronic message according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

A description of preferred embodiments of the invention follows.

Encrypting electronic message

FIG. 1 is a block diagram of a system for encrypting an electronic message according to the principles of the present invention. Referring to Fig. 1, a sender S100 wishes to encrypt an electronic message M101, such as an electronic mail or e-mail, to a receiver R100, but does not have a public key to use for receiver R100. In one embodiment, a sender client S101 authenticates itself to sender server S102 utilizing for example Challenge Handshake Authentication Protocol (CHAP) as described in the Internet Engineering Task Force (IETF) Request For Proposal (RFC) 1994, One-Time Password as described in RFC 1938, token card, Secure Remote Password Protocol (SRP) as described in RFC 2945, etc. Sender client S101 sets up a secure channel to sender server S102, using a secret session key negotiated with sender server S102 utilizing a secure key negotiation protocol based on Diffie-Hellman. In another embodiment, Transport Layer Security (TLS) protocol as described in RFC 2246 and RFC 3546 can be used for authentication and setting up a secure channel between sender client S101 and sender server S102. Sender client S101 securely sends e-mail electronic message M101 to sender server S102.

FIG. 2 is a flow diagram of a procedure for encrypting an electronic message according to the present invention. Referring to Fig. 2, at step 201, sender server S102 generates a new ad hoc asymmetric key pair comprising public key K101 and unencrypted private key K102, uniquely associated with both sender S100 and receiver R100. The size of the keys should be at least 2048-8192 bits for approximately a 128-bit security level.

At step 202, sender server S102 salts and stretches a sender secret S103 passphrase to 256 bits long for approximately a 128-bit security level, for use to encrypt unencrypted private key K102 into an encrypted private key K103 known only to sender S100. The salt used with sender secret S103 passphrase is stored alongside encrypted private key K103. The symmetric encryption functions for encrypting

unencrypted private key K102 are as described later below. Public key K101 and encrypted private key K103 make up an ad hoc key pair K100 that is uniquely associated with both sender S100 and receiver R100.

At step 203, sender server S102 creates an index value V101 that is uniquely associated with key pair K100 and is utilized for key retrieval. FIG. 3 is a block diagram illustrating an identity value that can be used to compute an index value utilized for key retrieval in one embodiment. Referring to Fig. 3, index value V101 can be simply an identity value 301 which is obtained from a concatenation of a unique sender identification S104 such as the e-mail address of sender S100, and a unique receiver identification R104 such as the e-mail address of receiver R100. In another embodiment, index value V101 is known only to sender S100, and is computed from a message authentication code (MAC) function, such as HMAC-SHA-256, with two arguments. One argument can be identity value 301. The other argument is a salted and stretched sender secret S103 passphrase.

Sender server S102 authenticates itself to key server KS101 utilizing for example PKI digital signature. Sender server S102 sets up a secure channel to key server KS101, using a secret session key negotiated with key server KS101 utilizing a secure key negotiation protocol based on Diffie-Hellman. In another embodiment, Transport Layer Security (TLS) protocol can be used for authentication and setting up a secure channel between sender server S102 and key server KS101.

At step 204, sender server S102 securely stores in key server KS101 index value V101, public key K101, and encrypted private key K103.

In another embodiment, key server KS101 stores index value V101 together with a set of key pairs. Each key pair is associated with a validity field such as a date stamp or a validity period. FIG. 4 is a block diagram illustrating a set of key pairs with validity fields. Referring to Fig. 4, sender server S102 generates, encrypts and stores a new ad hoc key pair K400 comprising a public key K401, an encrypted private key K403 and a validity field F401. Key pair K400 is used for encrypting new messages from sender S100 to receiver R100 after expiration of a validity field F101 associated

with ad hoc key pair K100. Expired key pair K100 is still stored in key server KS101 to be utilized for decrypting prior messages from sender S100 to receiver R100. A set of key pairs SKP400 comprising key pair K100 and key pair K400 is uniquely associated with both sender S100 and receiver R100. Index value V101 is uniquely associated with the set of key pairs SKP400.

In another embodiment, key server KS101 or other components of the system may charge a fee for access. In yet another embodiment, key server KS101 may be distributed over several key servers for redundancy, or may be implemented as a web service.

At step 205, sender server S102 encrypts e-mail electronic message M101 into an e-mail encrypted message M103 using a symmetric key E101, which is in turn encrypted into an encrypted symmetric key E102 by sender server S102 using asymmetric public key K101. Symmetric encryption functions that can be used include the counter (CTR) mode or the cipher block chaining (CBC) mode for the Rijndael cipher or the Twofish cipher. Rijndael is the Advanced Encryption Standard (AES) of the U.S. government. The size of symmetric key E101 should be at least 256-bit for approximately a 128-bit security level, which means that any attack will require approximately 2^{128} steps. In an alternate embodiment, symmetric key E101 is chosen to be $h(r)$ for some hash function h and a random $r \in Z_n$ where $(n, e=5)$ is public key K101, and r is encrypted into encrypted symmetric key E102 by raising r to the fifth power modulo n, as described on page 237 of Niels Ferguson and Bruce Schneier, *Practical Cryptography*, Wiley Publishing, Inc., Indianapolis, 2003.

In another embodiment, instead of a new ad hoc asymmetric key pair, a new ad hoc symmetric key with size and for symmetric encryption functions as described above is generated by sender server S102. The symmetric key is uniquely associated with both sender S100 and receiver R100, encrypted and known only to sender S100 as described above, stored in key server KS101 with index value V101 used for key retrieval as described above, and used directly to encrypt electronic messages to receiver R100.

Sender server S102 sends an encrypted electronic message M102 comprising encrypted symmetric key E102 and e-mail encrypted message M103 to a receiver server R102 through an insecure channel. If sender server S102 and receiver server R102 act as mail transfer agents, the Simple Mail Transfer Protocol (SMTP) can be used to transfer encrypted electronic message M102 as a multi-part e-mail. Sender server S102 sends public key K101 for local storage in sender client S101 to be utilized in encrypting future messages from sender S100 to receiver R100. In the alternative embodiment where a validity field is associated with key pair K100, public key K101 expires in sender client S101 when key pair K100 expires.

Decrypting electronic message

Referring to Fig. 1, receiver R100 wishes to decrypt encrypted electronic message M102 from sender S100, but does not have a corresponding private key to use for decryption. FIG. 5 is a flow diagram of a procedure for decrypting an electronic message according to the present invention. Referring to Fig. 5, at step 501, receiver R100 authenticates itself to sender S100. In one embodiment, a receiver client R101 authenticates itself to receiver server R102 utilizing for example Challenge Handshake Authentication Protocol (CHAP), One-Time Password, token card, Secure Remote Password Protocol (SRP), etc. Receiver client R101 sets up a secure channel to receiver server R102, using a secret session key negotiated with receiver server R102 utilizing a secure key negotiation protocol based on Diffie-Hellman. In another embodiment, Transport Layer Security (TLS) protocol can be used for authentication and setting up a secure channel between receiver client R101 and receiver server R102. Receiver server R102 in turn authenticates itself to sender server S102 utilizing for example PKI digital signature, which completes the authentication of receiver R100 to sender S100.

Receiver server R102 sets up a secure channel to sender server S102, using a secret session key negotiated with sender server S102 utilizing a secure key negotiation protocol based on Diffie-Hellman. Sender server S102 authenticates itself to key server

KS101 utilizing for example PKI digital signature. Sender server S102 sets up a secure channel to key server KS101, using a secret session key negotiated with key server KS101 utilizing a secure key negotiation protocol based on Diffie-Hellman. In another embodiment, TLS protocol can be used for authentication and setting up a secure channel between receiver server R102 and sender server S102, or between sender server S102 and key server KS101.

At step 502, sender server S102 derives an index value V101 from identity value 301, as previously described above, that is uniquely associated with key pair K100, key pair K100 being uniquely associated with both sender S100 and receiver R100. In another embodiment, index value V101 is known only to sender S100, and is derived from a MAC function with identity value 301 as one argument, and salted and stretched sender secret S103 passphrase as the other argument, as previously described above.

At step 503, sender server S102 retrieves via secure channel encrypted private key K103 that is stored in key server KS101 by using index value V101, encrypted private key K103 known only to sender S100.

In the alternative embodiment where a validity field is associated with a key pair, referring to Fig. 4, key server KS101 serves up set of key pairs SKP400 comprising key pair K100 and key pair K400 associated with index value V101. Sender server S102 selects the correct encrypted private key K403 based on the date of encrypted electronic message M102 being within the valid period of validity field F401 for key pair K400.

In another embodiment, key server KS101 or other components of the system may charge a fee for access. In yet another embodiment, key server KS101 may be distributed over several key servers for redundancy, or may be implemented as a web service.

At step 504, encrypted electronic message M102 is decrypted in three sub-steps by utilizing encrypted private key K103. Encrypted electronic message M102 comprises encrypted symmetric key E102 and e-mail encrypted message M103. Firstly, sender server S102 salts and stretches sender secret S103 passphrase to decrypt

encrypted private key K103 into unencrypted private key K102. The symmetric encryption functions for decrypting encrypted private key K103 are as previously described above. The salt used with sender secret S103 passphrase is stored alongside encrypted private key K103. Receiver server R102 securely obtains unencrypted private key K102 from sender server S102. Secondly, receiver server R102 uses unencrypted private key K102 to decrypt encrypted symmetric key E102 into symmetric key E101. Thirdly, receiver server R102 uses symmetric key E101 to decrypt e-mail encrypted message M103 into e-mail electronic message M101.

In the alternative embodiment where a symmetric key, instead of an asymmetric key pair, is generated, encrypted and stored by sender S100, and used directly to encrypt electronic messages to receiver R100, encrypted electronic message M102 is just e-mail encrypted message M103 and is decrypted in only two sub-steps at step 504, after the encrypted symmetric key is retrieved from key server KS101 at step 503. Firstly, sender server S102 decrypts the encrypted symmetric key into an unencrypted symmetric key, as described above. Receiver server R102 securely obtains the unencrypted symmetric key from sender server S102. Secondly, receiver server R102 uses the unencrypted symmetric key to decrypt e-mail encrypted message M103 into e-mail electronic message M101.

Receiver client R101 uses Post Office Protocol (POP) or Internet Message Access Protocol (IMAP) to obtain e-mail electronic message M101 via secure channel from receiver server R102. Receiver R100 receives decrypted e-mail electronic message M101.

It will be apparent to those of ordinary skill in the art, that methods involved in the present invention may be embodied in a computer program product that includes a computer usable medium. For example, such a computer usable medium can consist of a read only memory device, such as a hard drive or a computer diskette, having computer readable program code stored thereon.

It is understood that the receiver, sender and key server can be separate hardware components and each include a separate processor. Alternatively, the sender and key server can be components in the same system.

While this invention has been particularly shown and described with references to preferred embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the scope of the invention encompassed by the appended claims.